Flipping the Script

Becoming your attackers boogeyman
Before we get started
BRUCON
SPRING TRAINING
22 - 24 APRIL 2015
3-day courses by renowned experts

BRUCON
SECURITY TRAINING
5 - 7 OCTOBER 2015
3-day courses by renowned experts

BRUCON
HACKING FOR BEER

BRUCON
SECURITY CONFERENCE
8 - 9 OCTOBER 2015
2-day conference
featuring outstanding security presentations and workshops

www.bruccon.org
HI...I’m Chris
Disclaimer
Trigger Warnings

- Loud Anoying American
- Cursing
- Racism
- Religious Prejudice
- Sex
- Drugs
- Daddy / Abandonment issues
- Socio Economic Hate crimes
- Thin Skin
- Lack of sense of humor
- Sexual orientation
- Sexism
- Violence
- Vomiting
- Abuse
- Truth
- Fear
- Honesty
- Facts
- Emotions
- Tears
I'm Chris

AKA

cnickerson@laresconsulting.com

https://vimeo.com/laresconsulting

http://www.scribd.com/LaresExoticliability.com

@indi303

http://www.scribd.com/Lares

https://vimeo.com/laresconsulting
You Can Stop Compulsive Shopping And Over-Spending

Book An Appointment »
Or visit our online shop »

Hypnotherapy and NLP to Help You Stop Compulsive Shopping,
And take control of your overspending.
How much better will you feel,
When everything is under your control
Overcome your shopping addiction,
Hypnotherapy and NLP provides the cure.

Why Am I Addicted To Shopping?
Two reasons:
Either:
You feel bad (bored or anxious or angry or depressed or desperate etc) and the "bad" feeling so you go and shop. Often there is a 'good feeling' associated with
SHIT'S ON FIRE, YO
You can't beat having friends like the Lares team whose amazing Badge System work makes this possible!
PENTEST KING
6 GREAT MODELS TO CHOOSE FROM! A TEST FOR ANY BUDGET!

If you’re in the market for a new penetration test, look no further!

Level 1 – THE CLASSIC
This classic is sure to pretend to do something!

Level 2 – SMASH AND GRAB!
Get ready to have your network DESTROYED!!!!
Features:
- No regard for your business!
- Huge reports
- Scanners, scanners, scanners!

Level 3 – THE PACIFIER
You’ll get a great report every time (that doesn't mean everything is ok...)
Features:
- Might sell or service your office printer!
- Won't break anything!
**Level 4 – THE RFCist**
The tester knows EVERYTHING! Except the why part!
Features:
  - Technical genius
  - Anti-social

Your score: **100!**

**Level 5 – THE AUDITOR**
After careful risk analysis, your score is.....!
Features:
  - Tight, neat packages
  - No technical know-how
  - Lots of letters after their names

**Level 6 – THE RICH KID**
They spent all their money on this tool... It's got to work!
Features:
  - Loves buzzwords!
  - Includes really expensive accessories

All of these products come with absolutely no guarantee whatsoever and the purchaser of these products should buy at his/her own risk...
Custom Services

OSINT
SIGINT
TSCM/ Bug Sweeping
Exploit Development
Tool Creation
Attack Planning
Offensive Consultation
Adversarial Intelligence
Competitive Intelligence
Attack Modeling
Business Chain Vuln Assessments
Custom Physical Bypass Tool Design
Reverse Engineering
Other stuff I can’t write down...
Your PowerPoint presentation makes Jesus cry.
GET TO WORK

YOU AREN'T BEING PAID TO BELIEVE IN THE POWER OF YOUR DREAMS.
• 80,000 security incidents and more than 2,000 data compromises from 61 countries.
• The top three industries affected are the same as previous years: Public, Technology/Information, and Financial Services.
• In 70% of the attacks where we know the motive for the attack, there’s a secondary victim
• 23% of recipients now open phishing messages and 11% click on attachments
Figure 5.
The Defender-Detection Deficit
The common denominator across the top four patterns – accounting for nearly 90% of all incidents – is people.
MAXIMUM SECURITY ENTRANCE
What do we do to try and DEFEND?

Buy stuff
- Firewalls
- WAF
- IDS/IPS
- AV
- SIEM
- Etc...

Test our stuff
- Conduct Audits
- Do “PenTests”
- Vuln scanning?
- Hire 3rd parties
- Hire industry “Experts”
And what happens?

WE STILL GET HACKED ALL THE TIME!!!!!!!
HERE

THERE?
Stories from the OTHER SIDE

When attackers DON'T WIN! Because your infosec is FORCE is STRONG
The following things are a brief view of how customers have DEFENDED their networks and made it HURT for us.
GOOD SECURITY PROGRAMS ARE BUILT IN AND NOT BOLT ON
External Defenses

Sounds cool if you buy them and actually use them.
Rule #1 DON’T TALK TO STRANGERS

- Implemented blocks from all emerging threats lists
- Honeypots that if SCANNED or traffic was sent to, that IP was blocked. FOR GOOD.
- External SIEM integration that correlated logins. *Magic* the same address tries more than 3 usernames in an APP or SMPT it is banned for a certain time, if it happens after timeout, its banned for good
- Constant monitoring and baseline analysis of open ports. If it changed, a SEV1 ticket was created.
- Port scanning bans.
- Injection Bans
- Rejection of specific user agent strings (most tools out there have specific UA strings).
- Test it all until BLOCK mode WORKS! Monitor mode will just make you feel bad when u go back to your logs and see WHEN you got owned
- Big data like a boss. DO THREAT INTEL IN HOUSE!!!!
- Protect your OSINT (anonymize info like DNS records)
Quick fixes

Tons of free stuff out there to get you started.

- Drupal honeypot: [https://www.drupal.org/project/honeypot](https://www.drupal.org/project/honeypot)
- External honeypot starter [https://www.binarydefense.com/project-artillery/](https://www.binarydefense.com/project-artillery/)
- Tools to monitor open ports [https://github.com/subinacls/Filibuster](https://github.com/subinacls/Filibuster)
- Check your osint / attack surface and threat landscape [http://www.spiderfoot.net/](http://www.spiderfoot.net/)
Phishing is for kids
#2 If you are going to talk, be sure you know who it is

- Disable SMTP verify/validation
- Mailer verification (USE SPF)
- Use Mail filtering solutions that can intercept ALL mail protocols
  Encrypted and unencrypted
- Strict enforcement of Site Classification
- Analysis of certificate age and domain age “marination”
- Inspect all attachments and disallow all attachments except for a very
  specific set which have mitigating controls at the host or can be used in a
  sandboxed viewer.
- Browser based controls whitelisting 3rd party loaders like java, flash etc...
  (or disabling all together)
- Verification of sender identity
- USE DNS ANALYSIS
- Don’t forward DNS. Split DNS is not hard
Quickies

- Enable SPF
- Implement spamcop and other blocking lists
  https://www.spamcop.net/fom-serve/cache/291.html
  https://www.spamhaus.org
- Implement a Mail inspection gateway Preferably cloud and local
- Check security setting of SMTP/SPF/DNS
  http://www.dnssy.com/
- Create Split DNS don’t allow forwarding and use only the validated internal resolver.
  http://shorewall.net/SplitDNS.html
- Create automated Phishing reporting process in client or train users on process to submit
- Phish the users, test them, train them. And UPDATE your new hire training to include how to defend.
Internal Defenses

They ARE gonna get in, so knowing that

WHAT U GONNA DO ABOUT IT?
#3 Your internal network is a HOSTILE environment. Treat it as such

- Monitor inside MORE than outside.
- Portscan inside = Block and SEV1 IR response
- Segmentation of all servers from users.
- Create Classified zones, These will require 2 factor auth to a Jump box. Only jump box will be allowed to get into secured zone. Or Create VPN from user desktop directly into the Environment
- NEVER use VPN Pools. Always tie a user to a specific ip address and firewall rule limit ALL users to resources needed.
- Alert on ALL network device configuration change IMMEDIATELY.
- Use Netflows or other traffic analysis to identify top talkers and tune to find future anomalies
- Set up “HoneyNets”
- LOCK DOWN YOUR CONFIGS!!!!!!!
- Remove your default route and intercept all HTTP/S
Quick hits

- Set up your AV to disallow/ban anything port scanning
- Segment and firewall protect ALL servers from user segments
- Tune internal IDS to look for port scans and inappropriate user to server traffic. Also to identify protocols that shouldn’t be used (ex. DNS traffic to things other than the registered internal DNS)
- Restrict network device management to only validated addresses of network engineers OR setup mgmt. network that Engineers MUST vpn into.
- Audit your configs [https://github.com/pello/routerdefense](https://github.com/pello/routerdefense) [https://www.titania.com/nipperstudio](https://www.titania.com/nipperstudio)
Workstations are for WORK
#4 Users have the ability to **use** the companies resources.

- Only add user accounts through secured methods. **DO NOT USE GPO's that have cPassword or add accounts with cleartext values.**
- Users should only be allowed to go to categorized sites. Any/all other traffic must be denied.
- Whitelist approved and managed software.
- Disallow Local admin privs
- Do NOT let local admins to log on remotely
- Randomize ALL local admin passwords
- Maintain internal software reports for updates
- Manage all the things
- Host based firewalls, IDS, and behavioral analysis
- **SCAN ALL HOSTS** for vulnerabilities on a regular basis
Quickies

- Manage local admin passwords with a commercial solution or some of the open sources. Microsoft LAPS

- Create GPO’s to whitelist or blacklist services

- Remove admin rights

- Deploy anti exploitation defenses EMET

- Harden your devices. Linux, AIX, BSD, Etc.. hardening

- Enable hardening locally with detection and protection

- Use Authenticated Scans to inventory software, find non compliant software and define hardening.

- Harden default images
It's a SERVER...

Make it serve you.
#5 Servers have a specific purpose

- Do not install workstation software on a SERVER. Office, Adobe Acrobat....etc.

- Most of them do NOT need to connect to the internet. Not only does this mean NO access with firewall it means, unless the product would require an exception... NO BROWSER!

- Manage updates centrally and in house

- Segment, Segment, Segment..... SEGMENT THE DAMNED SERVERS!!!!!!!

- Standard image should have NO additional services installed and build guidelines should be followed before release.
Quickies

- Remove all non essential services from servers RIGHT AWAY. They will run faster and more secure.
- Disallow install of any readers, office type programs or all workstation software in server hardening policy.
- Run Full AV on EVERY server.
- If you can’t get ids.ips for your servers try opensource like OSSEC [http://www.ossec.net/](http://www.ossec.net/)
- Use DLP [https://code.google.com/p/opendlp/](https://code.google.com/p/opendlp/)
- Disallow all non authenticated services.
- Do not allow the use of local accounts to log in remotely (that includes you SQL!!! No local sql accounts.. Integrate it)
- Make sure all report to the SIEM for security and login events.
Two Content Layout with Table

- First bullet point here
- Second bullet point here
- Third bullet point here

<table>
<thead>
<tr>
<th></th>
<th>Group A</th>
<th>Group B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class 1</td>
<td>82</td>
<td>95</td>
</tr>
<tr>
<td>Class 2</td>
<td>76</td>
<td>88</td>
</tr>
<tr>
<td>Class 3</td>
<td>84</td>
<td>90</td>
</tr>
</tbody>
</table>
#6 Awareness > Knowledge

- Create Security Event Management Environments
- Implement logging on ALL servers and eventually specific workstation events.
- Consolidate logging
- Have packet capture capabilities on the fly in ALL areas
- Looks at the hotness of attack surfaces and start to build defenses based on techniques used in offense. (ex. WMI trend)
Quick hits

- Set up IDS/IPS and have it report to a consolidated platform
  [http://blog.securityonion.net/p/securityonion.html](http://blog.securityonion.net/p/securityonion.html)
  [https://www.bro.org/](https://www.bro.org/)

- Set up logging and have it report to a consolidated platform

- Make it easy for yourself. Help correlate from multiple sources.
  [https://bammv.github.io/squil/](https://bammv.github.io/squil/)

- Fireeye-FLARE Windows WMI-IDS
WMI (WHY?)

1. An attacker uses WMI as a persistence mechanism • Effect: Instances of __EventFilter, __EventConsumer, and __FilterToConsumer Binding are created. An __InstanceCreationEvent event is fired.

2. The WMI Shell utility is used as a C2 channel • Effect: Instances of __Namespace objects are created and modified. Consequently, __NamespaceCreationEvent and __NamespaceModificationEvent events are fired.

3. WMI classes are created to store attacker data • Effect: A __ClassCreation Event event is fired.

4. An attacker installs a malicious WMI provider • Effect: A __Provider class instance is created. An __InstanceCreationEvent event is fired.

5. An attacker persists via the Start Menu or registry • Effect: A Win32_StartupCommand class instance is created. An __InstanceCreationEvent event is fired.

6. An attacker persists via other additional registry values • Effect: A RegistryKeyChangeEvent and/or RegistryValueChangeEvent event is fired.

7. An attacker installs a service • Effect: A Win32_Service class instance is created. An __InstanceCreationEvent event is fired.
Shout out to all my Basic bitches.

10 PRINT "HOLLA"
20 GOTO 10
RUN
There was a spider, I panicked.

But I think it's gone now.

Get your IR game in order
#7 In order to say you have an information security program you need to have an Incident response plan.

- Humans must be assigned to this plan and the tasks in it
- Security response center must have defined plans, SOP’s, and most of all a fully capable SLA to the business on risk response/identification
- Active defenses to stop attack in progress
- Forensic/ malware analysis on the fly and manual
- Coordination with all teams to have real time response.
- Defined skillsets of all team members to be sure the right skill for project.
Quick ways?

- Build a proper IR team. Define skills and roles to be played
- Setup an IR action group (from all of IT and the business)
- Create defined IR plans that can be run as part of DR plans
- Build an IR Team Sandbox toolkit / lab
  https://zeltser.com/build-malware-analysis-toolkit/
- Build an Incident response platform
  https://github.com/google/grr
  http://techblog.netflix.com/2015/05/introducing-fido-automated-security.html
- https://www.bestpractical.com/rtir/
- https://www.mediawiki.org/wiki/Download
DONE WITH MY PRESENTATION

NOW I HAVE TO ANSWER QUESTIONS
I'm Chris
AKA
@indi303
cnickerson@laresconsulting.com

Exoticliability.com

http://www.scribd.com/Lares
http://www.scribd.com/Lares
https://vimeo.com/laresconsulting